BBN REPORT NO. 3310

May 1976

MESSAGE TECHNOLOGY RESEARCH AND DEVELOPMENT

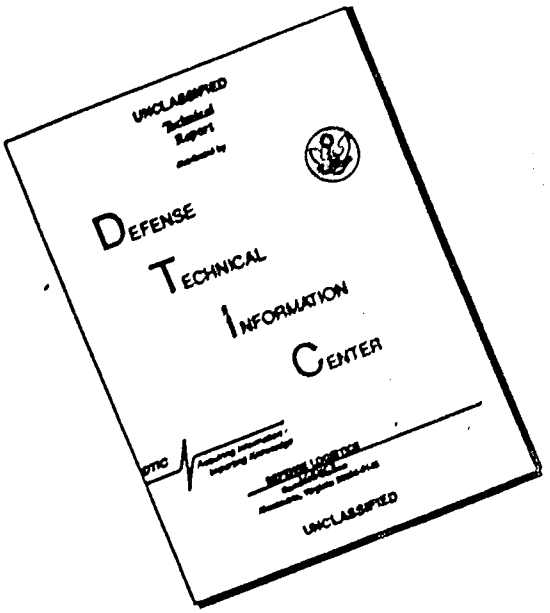
Quarterly Progress Report No. 1

2 January 1976 to 2 April 1976

PROJECT HERMES

Bolt Beranek and Newman Inc. 50 Moulton Street Cambridge, Mass. 02138

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER BBN REPORT NO. - 3310	2 GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4 TITLE (and Subtitle) MESSAGE TECHNOLOGY RESEARCH AND DEVELOPMENT.		5 TYPE OF REPORT & PERIOD COVERED Quarterly Progress 1/2/76 - 4/2/76
		6. PERFORMING ORG. REPORT NUMBER
7 AUTHOR(s) J. Burchfiel T. Myer		8 CONTRACT OR GRANT NUMBER(s) MDA903-76-C-0212, ARPA Order-3161
9 PERFORMING ORGANIZATION NAME AND ADDRESS Bolt Beranek and Newman Inc. 50 Moulton Street Cambridge, Massachusetts 02138		10 PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11 CONTROLLING OFFICE NAME AND ADDRESS		12. REPORT DATE May 1976 13 NUMBER OF PAGES 22
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16 DISTRIBUTION STATEMENT (of this Report)
Distribution of this document is unlimited. It may be released to the Clearinghouse, Department of Commerce for sale to the general public.

17 DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

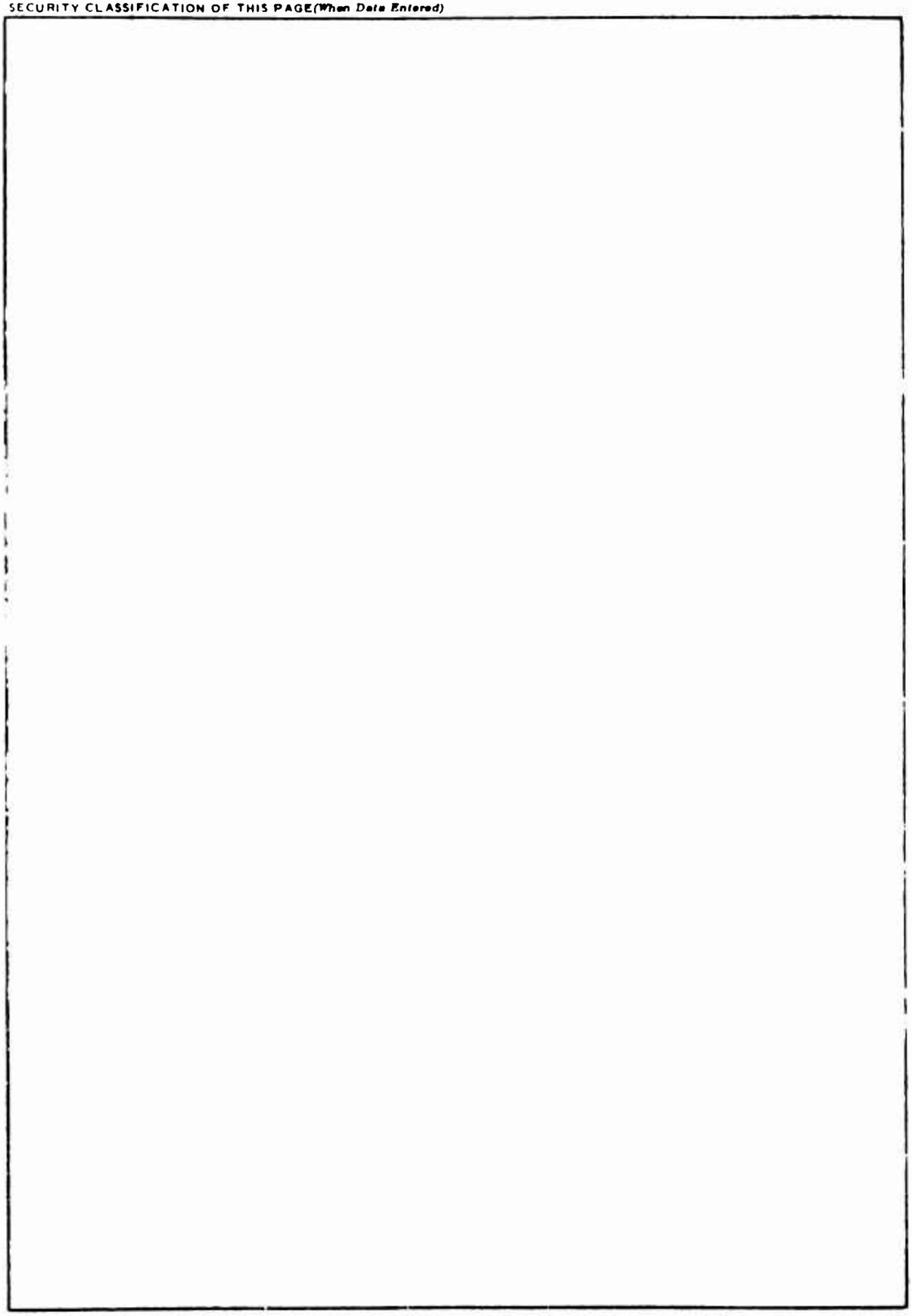
18 SUPPLEMENTARY NOTES
This research was supported by the Defense Advanced Research Projects Agency under ARPA Order No. 3161

19 KEY WORDS (Continue on reverse side if necessary and identify by block number)
Hermes
Message Processing
Tenex Security
CINCPAC Test

20 ABSTRACT (Continue on reverse side if necessary and identify by block number)
This report describes BBN efforts in the continuing development of the HERMES message-processing system, with respect to system design, security requirements and preparations for the DARPA/NAVY/CINCPAC interactive test.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

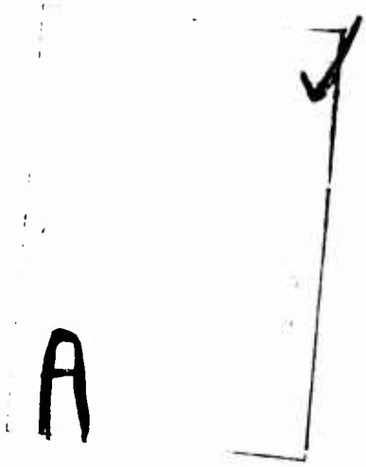


BBN Report No. 3310 May 1976

MESSAGE TECHNOLOGY RESEARCH AND DEVELOPMENT

Quarterly Progress Report No. 1

2 January 1976 to 2 April 1976



This research was supported by the Defense Advanced Research Projects Agency under ARPA Order No. 3161 Contract No. MDA903-76-C-0212

TABLE OF CONTENTS

I. INTRODUCTION TO MAILSYS/HERMES

This report covers progress in message technology under the contract "Message Technology Research and Development" for the period 2 January 1976 through 2 April 1976.

This work is a continuation of work on MAILSYS/HERMES performed under the ARPA Contract "Distributed Computation and TENEX Related Activities" during 1975.

The work leading up to this report is covered in the following earlier quarterly progress reports.

DISTRIBUTED COMPUTATION AND TENEX-RELATED ACTIVITIES

QPR No. 1	1 Nov 74 - 31 Jan 75	BBN Report No. 3012
QPR No. 2	1 Feb 75 - 30 April 75	BBN Report No. 3089
QPR No. 3	1 May 75 - 30 July 75	BBN Report No. 3117
QPR No. 4	1 Aug 75 - 30 Oct 75	BBN Report No. 3210
QPR No. 5	1 Nov 75 - 30 Jan 76	BBN Report No. 3257

QPR No. 5 covered MAILSYS/HERMES activities only through 1 January 1976.

Our major effort during the January-March period has been to move ahead systematically with the development and refinement of MAILSYS/HERMES Version 2, following the phased development program reported in QPR No. 4 listed above. During this period, the name "MAILSYS" has been phased out in favor of "HERMES".

Human Factors Evaluation

Human factors evaluation of each successive modification to

Hermes has been accomplished, and the results have been used to guide the design of present and future versions of the system. Versions 2.4 and 2.5 of Hermes were implemented and given limited release during this period, as described in the following pages.

Data Management and On-Line Storage

We have greatly improved the ability of HERMES to store information of benefit to the user from one HERMES session to the next. The user's Profile can now store filters, templates, and switch settings. Special index files, created by HERMES for all message-files, store user-created sequences or subsets of messages in the message-file and "parsing" information that allows Hermes to start up and search message-files with less cost in computer time.

Documentation

On-line reference documentation for Hermes Version 2.4 was completed and documentation summary material was prepared. Work has continued on the development of tutorial documentation aimed at users with varying levels of sophistication.

Delivery System

Preliminary design has begun on a distributed delivery system which will act as a transmission mechanism and repository for messages. The delivery system will make use of MSG, an interhost interprocess communication facility for the National Software Works,

which has been developed at BBN under ARPA Contract.

Application-Level Security

With respect to security for Hermes on the level of users accessing individual messages, we explored several alternate plans. This preliminary design effort led to, and was superceded by, a new concept for a security system which will be reported in the next QPR.

Monitor Level Security

During this period, we have designed, coded, and demonstrated an experimental "encapsulator" for the TENEX system which provides an independent check on system protection. The encapsulator makes an independent determination of the security status of the user with respect to the files accessed, with protection assignable to directories, files or even extension or version sub divisions of files. The encapsulator will also make it possible for the user to be placed directly into HERMES (or any other program) immediately after Log-In, without gaining access to a top-fork Executive program.

Host-to-Host Security

In preparation for the CINCPAC test, we have designed a method of extending the ARPANET NCP Host-to-Host Protocol for use in a multi-level secure environment. The method chosen involves defining

a new Host-to-Host control message, which also contains the present byte-size match information.

LDMX Interface

Work on the LDMX interface has continued, with collaboration between BBN and NAVCOSSACT on the details of the LDMX/TENEX protocols. Programming of the TENEX portion of the protocols has been completed and has been demonstrated to NAVCOSSACT personnel.

Distan Test Preparation

The Human Factors group has continued consulting on HERMES design and has participated in plans for the DARPA/NAVY/CINCPAC test. We have agreed to work with NAVELEX and MITRE personnel to refine and sharpen a model of the impact of computer-based message technology on future Navy operations.

II. HERMES VERSION 2.4

We created HERMES Version 2.4 as a next stage beyond version 2.3, incorporating a number of corrections and improvements of the basic code.

A special version of HERMES 2.4 that implements DoD form DD-173 was installed at ISIA and OFFICE-1, on an experimental basis. This version contains special header and text fields duplicating those currently used in military messages.

The Describe documentation was updated to reflect HERMES Version 2.4 and a set of documentation summaries were prepared and made available on-line through Describe and as a booklet through the TENEX Exec.

III. HERMES VERSION 2.5

A. Automatic Stored Sequences

Stored sequences are a major new data management tool that was introduced in Hermes 2.5. Sequences are lists of message-numbers created and given names by the user, which can function as "file-folders" within a message-file. A sequence can be created by typing individual message-numbers or by performing a search with one or more filters on the message-file and creating a sequence of the result.

Permanent sequences allow the user to create sequences within a major message-file, such as MESSAGE.TXT;1, rather than using the FILE command to copy the messages physically into another message-file. The advantages are:

1. The same message-number may appear on any number of sequences without duplication of the physical message.

2. Sequences may be manipulated in many ways: combined according to Boolean functions, sorted, reversed, or erased, without disturbing the location of the original message in the message-file.

User-created sequences associated with a particular message-file are automatically saved until they are explicitly erased. The associated sequences automatically appear in the active environment when the message file is accessed. When messages are

deleted and expunged, all sequences are automatically updated to reflect the expunged messages and changed message numbers.

Sequences are now shown in the most concise form in which they can be typed in. Example:

```
>Create Sequence Jones<cr>
>Add 1,3,5,9,8,7,22:24,25:30<cr>
>>Show<cr>
1,3,5,9:7,22:30
>>
```

B. Compose Templates

Templates have been introduced into message composition, where their use is analogous to an "inversion" of their use in message output. The new compose templates allow the user to tailor his own set of prompts for message composition through use with the COMPOSE command.

Each field named in an input, or compose, template is presented to the user as a prompt for input to that field. The user may create his own compose templates with any desired selection of fields to be presented as prompts in any order. Other features of Compose templates allow the user to insert comments or label standard fields and insert prepared text into fields.

Quoted Strings

As in printing templates, quoted strings may be used to relabel fields or provide additional information.

Literal Field Content

We have introduced a new type of template item for use in Compose templates, to save user from having to type in repetitive information in a series of messages. Literal items insert a field, together with the contents of the field, in the outgoing message. When a Compose template is shown, a literal item appears as

literal [Cc: Jones, Smith]

A new current template, CTEMPLATE, is the default template for the COMPOSE command. Any template may be used as either a compose template or a printing template. The printing commands SURVEY, PRINT, LIST, and <LF> ignore any literal items in a template.

C. Spelling Correction

HERMEs now automatically corrects spelling mistakes in commands and names of objects.

D. Improved LIST Command

The LIST command now takes a template argument. The default template for LIST is a new current template named LTEMPLATE. The separation between messages in a Listed sequence is now under the control of a new template item "Separate", which inserts a formfeed or new-page signal (<CTRL-L>).

E. Improved Method for Storing Objects in the PROFILE

It is now much easier to edit the profile so as to save permanent SWITCH settings and user-created filters and templates. The EXPORT and IMPORT commands now work at the top command level in the active environment -- all of HERMES that is not Profile. The EXPORT command copies an object from the active environment into the Profile and stores in permanently under the same or a different name, at the user's option. The IMPORT command, used in the active environment, copies an object that exists in the Profile into the active environment.

It is now necessary to enter the PROFILE with the EDIT PROFILE command only to erase profile objects. However, it is still possible to create and edit filters and templates and change switch settings, in the second-level profile editor. the EXPORT command copies profile objects into the active environment, and the IMPORT command brings them from the active environment into the PROFILE.

F. Other Improvements

A number of other improvements have been incorporated in Hermes.

1. The SEND command now automatically returns the user to the top command level. This change has been made to reduce confusion about levels, and to make life easier for people who like to alternate between printing, filing, and deleting messages.

2. The top-level commands for creating messages are CREATE, and

EDIT CDRAFT. Top-level commands for prompted composition are COMPOSE, REPLY, FORWARD, and SUGGESTION. All of these commands automatically cause the user to enter the second-level Draft-Editor. When the user SENDS the message, he is automatically returned to top command level. If he wishes to return to top command level without SENDing the message, he may type DONE to the >> prompt. The CDRAFT is not erased.

3. The commands COMPOSE, REPLY, FORWARD, SUGGESTION, QUIT, and EXIT now warn there is unerased text in the CDRAFT and ask whether or not the user wishes to proceed.

4. In the SUGGESTION command, the message is no longer automatically sent as soon as the Text:-field is completed. Suggestion is now a prompted sequence, like Reply or Forward.

5. HERMES no longer locks the user out after <CTRL-C> or when the system crashes. The user may give the TENEX CONTINUE Command and recover after <CTRL-C>.

6. Three new switches have been added:

   a. The FROM-NAME SWITCH controls whether the FROM:-field contains the name of the Login or Connected Directory. (2 positions)

   b. The TEXT-FORMAT switch allows the user to set the system to automatically FORMAT the Text:-field, or not to FORMAT, or to ask whether to FORMAT. (3 positions)

   c. The TRANSMIT-NOW SWITCH allows the user to specify whether messages are to be transmitted immediately or queued. (3 positions)

7. Subcommands that override switches are still invoked TENEX-style by confirming the command with ,<cr> instead of <cr>. The subcommand prompt is now +>.

```
>Reply 37,<cr>
+>NoCopies<cr>
+><cr>
>
```

8. NEW messages are reported both at the top level and in the DRAFT-EDITOR. The automatic initial survey of new messages shows the message-no. of the CMESSAGE.

9. The FORWARD command now prompts for a subject:-field, which is entered as the first line of the Subject, before the automatically created subject line containing Author and Subject of the first forwarded message.

10. The New Check-Printer command queries the lineprinter queue in the <printer> directory, and prints a message "PRINTING IN PROGRESS" or "PRINTING NOT IN PROGRESS".

11. The FILE, MOVE and DELETE Commands now confirm that the action is completed by printing out the message-nos.

12. The "Delete" or "Rubout" key no longer has any function during text creation. This eliminates a serious problem of loss of input text due to spurious "rubout" signals for users with noisy lines.

13. Minor Changes: The FORMAT switch is renamed FORMAT-JUSTIFY. "Cleanup" is no longer used as a synonym for "Expunge". In the

Show command, objects of each type are displayed in the following order: Current, User-Created and Fixed. The fixed objects NULLSEQUENCE, NULLFILTER, and NULLTEMPLATE have been abolished as not needed.

IV. DOCUMENTATION

The documentation accessed by the DESCRIBE command was updated for HERMES 2.4. A booklet of summary documentation was prepared and made available on-line.

Work has continued on the development of tutorial documentation aimed at users of varying levels of sophistication. At the end of the reporting period, materials in preparation included:

A. A tutorial guide for novice users;

B. A User Guide covering all aspects of HERMES;

C. A short interactive on-line program to guide users to appropriate documentation;

D. An interactive, structured program that provides a conceptual map of the entire system.

V. NEW DELIVERY SYSTEM

We have begun preliminary design explorations into a distributed message delivery system which would make use of repositories of message at host computer sites rather than individual files in users' directories.

The new delivery system will require a facility for communicating between hosts and between processes running on different hosts. We at BBN have developed such a facility, MSG: The Interprocess Communication Facility for the National Software Works* (not to be confused with the network mail system, also called MSG).

We plan to use the MSG Interprocess communication Facility to support the new delivery system for Hermes.

Each host site would have a common repository of messages that would also act as part of the message transmission system. Users would be notified of their new messages by citations sent over the network, and any individual message would be retrieved and transmitted from one host site to another only when a user asked to look at the text of the message. After a message had been transmitted over the network at the request of one user, it would

---

* BBN Report No. 3237, "MSG: The Interprocess Communication Facility for the National Software Works (Preliminary), January 23, 1976, NSW Protocol Committee. ARPA Contract No. F30602-76-C-0094, ONR Contract No. 0014-75-C-0773.

become part of the message repository at the recipient's host computer. Any other recipient at the same host would thereafter retrieve his copy of the message from the local repository rather than from the sender's host repository.

Issues explored were how to move messages from one site to another, how to locate messages, and how to optimize the process by which the local repository compares Message-IDs and determines which messages are in the local store, and which must be transmitted over the network.

Details for further design work will be reported in the next QPR.

VI. SECURITY

A. Application-Programming-Level Security

In this quarter we worked through the early design stages of several alternate plans for security systems on the application programming level. Attention was focussed on the classification of various designs, dependent upon whether or not the header fields of the messages are classified, the system is to provide write-down capability, at different levels of restriction, and whether a uniform environment is to be implemented.

This work clarified the problems to be solved and resulted in a new design concept that supercedes the previous design concepts. The new work in application-programming-level security will be reported in the next QPR.

B. An Experimental Encapsulator for Access Verification at the System Monitor Level

During this quarter, we have designed, coded, and demonstrated an experimental Encapsulator for the TENEX system. This is a program that provides an independent check on system protection at the level of directories and files. The Encapsulator makes a determination of the security status of the user, independent of the regular TENEX protection system; protection is assignable directories, files, or even extension or version subdivisions of files.

Modifications to the TENEX system have been developed that

allow the Encapsulator to act on a per-user basis and decide which program, other than the EXEC, the user should perceive as being in the "top fork". The Encapsulator will create a pseudo top fork, run the selected program, which may be HERMES or any other program, in the pseudo top fork, and monitor any system calls so as to prevent the user accessing other selected parts of the TENEX facilities.

The Encapsulator makes it possible for the user to be placed directly into HERMES as soon as he has logged in, without having been given access to the TENEX Exec.

The Encapsulator maintains separate lists of readable and writable devices for each user. In the current implementation, this is only a read list and a write list, which are tuned for people using the HERMES system. This is the "independent reference" and is a model of what the file system should permit.

The Encapsulator is, to some extent, a detector of abnormal situations. If the "pseudo-top-fork" program fails to handle illegal read, write, and execute interrupts, the Encapsulator will note the interrupt and log out the job -- the only "safe" thing to do.

C. Implementation of AIM Security Enhancement Additions to TENEX at the System Monitor Level

The coding has been completed for the first set of AIM additions to TENEX. These are security enhancements in the TENEX which were designed jointly with MITRE and implemented at BBN. Implementation of the second set will be reported in the next QPR.

D. Extending the ARPANET NCP Host-To-Host Protocol for Use in a Multi-level Secure Environment

For the CINCPAC Interactive Message Systems Test, it will be necessary to have a security level associated with processes in the two (or more) computers and with the ARPANET connections between the hosts. This in turn requires extension of the Host-to-Host Protocol for use in a multi-level secure environment. Two protocols were investigated. One was rejected because of its inflexibility and difficulty of implementation.

The method chosen centers about defining a new host-to-host control message.

1. The new host-to-host control message contains the same information as STR (Code 2, "sender- to-receiver request for connection"), but has five more 8-bit bytes of security information in addition. The message is called "sender-to-receiver request for secure connection" (SSR) and is NCP op-code number 23 (octal).

2. The first of the additional five bytes contains four capability bits and a four-bit classification level. The following four bytes contain 32 compartment indicator bits. The most-significant (first sent) capability bit is the system security officer or "write-down" bit. The other three capabilities are not currently assigned. The four-bit classification level is coded 0 for Unclassified, 4 for Confidential, 10 for secret, and 14 for top-secret. None of the compartments have been assigned meanings at this date.

3. TENEX will check the security level information at the same time that it currently checks for connection byte-size match. A security level mismatch will cause the connection to be closed in the same way that a byte-size mismatch is treated. The failure will give an error indication to the local process.

VII. LDMX INTERFACE

We are continuing our collaboration with NAVCOSSACT on the protocols of the LDMX/TENEX interface.

1. Frank Ulmer has met with NAVOSSACT personnel to discuss the final details of the protocol problems. Also discussed were the requirements of the PDP-11 with respect to the TENEX/LDMX connections.

2. The final design for the TENEX portion of the protocols is complete.

3. The coding for the TENEX portion of the protocols has been completed. The implementation of the final design was accomplished without requiring further changes in the design.

4. All the programming for the communications process is debugged as well as it can be until an LDMX can be connected. The program has been tested by looping communications lines back into the program.

5. The completed programming has been demonstrated to NAVCOSSACT personnel.

VIII. HUMAN FACTORS

The Human Factors group has continued consulting on the design of HERMES commands and objects, and has participated in HERMES design meetings.

The Human Factors people participated at a NAVELEX meeting in Washington, D.C. on January 19-23, on the subject of planning for the DARPA/NAVY/CINCPAC military message experiment.

The Human Factors group has prepared a description of a CRT terminal interface to Hermes that would use the ISI protocols and be operated on the HP 2250A terminal. The specification is written from the user's perspective. It proposes to use terminal function keys for frequently used commands and to be compatible with existing user procedures operating from a printing terminal.

This paper has been released as HERMES Working Paper 5.1, "A Proposal for a CRT Display-Keyboard HERMES Interface", dated February 4, 1976.

Human Factors people met with R. Uhlig to discuss his plans for measuring system cost-effectiveness for DARCOM applications.

A meeting was held with C. Bergstrom, L. Klitzkie, E. Bersoff, C. Heitmeyer , et al to discuss our role in assessment of the impact of message system technology on future Navy operations. We agreed to work toward constructing a framework from which it might be possible to predict the changes that could be expected in Navy

message handling operations as a result of introduction of computer-based message technology. The framework would be derived from retrospective analysis of current uses of message systems, and from L. Klitzkie survey of the characteristics of message handlers.

A tentative model will be formulated prior to the CINCPAC Test and questionnaires prepared to supplement the data to be collected by MITRE for purposes of evaluating and refining, particularly with respect to the assessment of organizational impact. The framework and procedures used for assessing impact would then be used as new operations begin to introduce new message systems.

The long-range goal is to gradually refine and sharpen a model of the impact of the technology so that when large-scale implementation is planned, it will be possible to forecast the changes in organization, personnel requirements, job descriptions and work loads that would be associated with the introduction of computer-based message technology.